UNIVERSITI PUTRA MALAYSIA

EFFICIENT AND SECURED COMPRESSION AND STEGANOGRAPHY TECHNIQUE IN WIRELESS SENSOR NETWORK

AMMAR YASEEN TUAMA

FSKTM 2016 24

EFFICIENT AND SECURED COMPRESSION AND STEGANOGRAPHY TECHNIQUE IN WIRELESS SENSOR NETWORK

By

AMMAR YASEEN TUAMA

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfillment of the Requirements for the Degree of Master of Science

April 2016

DEDICATIONS

I dedicate my thesis to my parents and wife. A special feeling of gratitude to my loving parents. I also dedicate this work to my supervisory comittee, Dr. Mohamad Afendee who guide me throughout the study period, Dr. Abdullah and Dr. Zurina for their advices and guidance. I will always appreciate all they have done.
I dedicate this work and give special thanks to all my friends who support and help me to improve and complete this work.

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Science

EFFICIENT AND SECURED COMPRESSION AND STEGANOGRAPHY TECHNIQUE IN WIRELESS SENSOR NETWORK

By

AMMAR YASEEN TUAMA

April 2016

Chairman: Mohamad Afendee Bin Mohamed, PhD
Faculty : Computer Science And Information Technology

Wireless Sensor Networks (WSNs) have emerged as one of the most promising solutions for wireless communication. They can be used in a wide variety of applications ranging from military tasking, healthcare servicing, disaster prediction and indoor positioning. However, the need to use less complex and low-cost sensor device results in constraints in computational power, communication bandwidth, and operational energy. In fact, the growing demands for new and much complex WSN applications require optimising both efficiency and security of data communication archetype in order to counterbalance their intrinsic limitations. In this study, to address these issues, we propose two techniques, one for minimising the transmitted data size in order to improve the efficiency of the WSN and the other for securing the sensed data transmission. First, the new data compression algorithm is proposed for compressing sensed data before it gets transmitted to the sink. The proposed solution is designed to be less complicated, low energy consumption and resource efficient with the ability to provide a lossless compression for a variety of data size. We analyse the solution and compare with a range of well-known algorithms in terms of compression ratio, memory usage, the number of instructions, compression speed and energy consumption. Two datasets have been used in the experiment, generated data set and Harvard Sensor Lab data set, in order to validate the performance of the proposed solution. The result shows that the proposed solution can compress both small and large data efficiently with up to 60% compression rate, 10 times faster compression speed and 4 times lower energy consumption compared to existing algorithms. Second, an improved steganographic algorithm based on the infamous Least Significant Bit (LSB) is proposed for hiding the sensed data scheduled for transmission. The proposed solution comes with low complexity and is used to enhance the security of the standard LSB algorithm by replacing an originally less secured sequential data hiding with a random pixel selection. This random pixel selection is achieved via the use of an Elliptic Curve equation. In terms of security,

the proposed solution is studied against brute-force attacks and the analysis shows that the new algorithm can withstand this type of attack with an ample amount of hiding possibilities that make the process of retrieving the message extremely difficult. Furthermore, some analyses on hiding quality show that our algorithm retains the cover image quality as high as that of standard LSB algorithm. Apart from being able to work with various limitations of the sensor node, both techniques can preserve the resource without sacrificing the performance of the nodes, security level of the data and lifetimes of the WSN, and therefore are good candidates for future implementation into the sensor node.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

TEKNIK PEMAMPATAN YANG CEKAP DAN STEGANOGRAFI YANG SELAMAT UNTUK RANGKAIAN PENGESAN TANPA WAYAR

Oleh

AMMAR YASEEN TUAMA

April 2016

Pengerusi: Mohamad Afendee Bin Mohamed, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Rangkaian Pengesan Tanpa Wayar (RPT) telah muncul sebagai salah satu penyelesaian yang paling menakjubkan untuk komunikasi tanpa wayar. Mereka boleh digunakan dalam pelbagai aplikasi termasuk tugasan ketenteraan, khidmat kesihatan, ramalan bencana dan kedudukan tertutup. Walau bagaimanapun, keperluan kepada penggunaan peranti pengesan yang mudah dan murah telah menyebabkan kekangan kepada kuasa pengiraan, lebar jalur komunikasi, dan tenaga operasi. Malahan, permintaan yang semakin meningkat kepada aplikasi RPT yang baru dan lebih kompleks memerlukan pengoptimuman dalam kecekapan dan keselamatan asas komunikasi data dalam usaha untuk mengimbangi batasan dalaman mereka. Dalam kajian ini, kami mencadangkan dua teknik baru, satu untuk mengurangkan saiz data yang dihantar dan satu lagi untuk keselamatan penghantaran data yang terkumpul. Pertama, satu algoritma baru pemampatan data dicadangkan bagi tujuan memampatkan data yang dikesan sebelum ia dihantar ke stesen penerima. Penyelesaian yang dicadangkan direka supaya kurang kompleks, menggunaan tenaga yang rendah dan sumber yang cekap dengan keupayaan untuk menyediakan pemampatan tanpahilang untuk pelbagai saiz data. Kami menganalisa penyelesaian tersebut dan membandingkan dengan pelbagai algoritma terkenal yang lain dari segi nisbah mampatan, kelajuan mampatan, dan penggunaan tenaga. Hasil kajian menunjukkan bahawa penyelesaian yang dicadangkan boleh memampatkan sebarang saiz data secara cekap sehingga mencapai kadar mampatan sebanyak 60%, kelajuan mampatan sebanyak 10 kali ganda dan penggunaan tenaga sebanyak 4 kali lebih rendah berbanding algoritma yang sedia ada. Seterusnya, satu algoritma steganografi baru berasaskan Bit Kurang Penting (BKP) yang terkenal dicadangkan untuk penyembunyian data yang dikesan, yang dijadualkan untuk penghantaran. Penyelesaian yang dicadangkan direka dengan kerumitan yang rendah, dan digunakan untuk meningkatkan tahap keselamatan algoritma piawaian BKP dengan menggantikan kaedah penyembunyian data berjujukan asal yang kurang selamat dengan pemilihan piksel rawak. Pemili-

han piksel rawak ini dapat dicapai melalui penggunaan suatu persamaan lekuk eliptik. Dari segi keselamatan, penyelesaian yang dicadangkan dikaji terhadap serangan kuasa-kasar dan analisis menunjukkan bahawa algoritma baru boleh menahan jenis serangan ini dengan jumlah kemungkinan penyembunyian yang besar di mana proses mendapatkan mesej menjadi amat sukar. Tambahan pula, beberapa analisa ke atas kualiti penyembunyian menunjukkan bahawa algoritma kami dapat mengekalkan kualiti imej penutup setinggi algoritma piawaian BKP. Selain daripada kebolehan bekerja dengan pelbagai batasan alatan pengesan, kedua-dua teknik tersebut dapat memelihara sumber sedia ada tanpa mengorbankan prestasi alatan, tahap keselamatan data dan hayat RPT, dan oleh itu ia adalah calon yang sesuai untuk dilaksanakan dalam alat pengesan masa depan.

ACKNOWLEDGEMENTS

I came to this beautiful country three years ago to pursue M.Sc study in Computer Science. I have been getting acquainted with all those lovely professors and colleagues, who inspire me, teach me and bring a lot of happiness to my life.

First and foremost, Alhamdulillah for giving me the patience and strength, and inspired me to completing this work. All grace and thanks belong to Almighty Allah.

At this important moment in my life, I would like to express my sincerely thanks to people who taking an important part in my life. To who sacrificed their own happiness, just so that I could be happy. Who opened their arms for me when the world closed its doors on me. I wish at these moments you are with me. Thanks my father and mother. A great thanks for my wife, my love, who fighting with me to reach my dream.

I take this opportunity to record my great thank to my advisor, who has the best heart in the world, Dr. Mohamad Afendee for his inspiration, motivation, and guidance. With him, I haven't felt alone on the way of studying because, in my deep heart, I know that he is with me.

I would also thank my co-advisor Dr. Abdullah Muhammed and Dr. Zurina Mohd Hanapi for generously offering their time, support, and good will throughout the preparation and review of this document.

I certify that a Thesis Examination Committee has met on 28 April 2016 to conduct the final examination of Ammar Yaseen Tuama on his thesis entitled "Efficient and Secured Compression and Steganography Technique in Wireless Sensor Network" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Master of Science.

Members of the Thesis Examination Committee were as follows:

Zuriati bt Ahmad Zukarnain, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Azizol b Hj Abdullah, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Mustafa Mat Deris, PhD
Professor
Faculty of Computer Science and Information Technology
Universiti Teknologi Tun Hussein Onn
(External Examiner)

ZULKARNAIN ZAINAL, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 26 July 2016

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Master of Science.

The members of the Supervisory Committee were as follows:

Mohamad Afendee Bin Mohamed, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairperson)

Abdullah Bin Muhammed, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Zurina Binti Mohd Hanapi, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

BUJANG KIM HUAT, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: _____ Date: _____

Name and
Matric No: Ammar Yaseen Tuama / GS38988

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia(Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: _____
Name of Chairman of
Supervisory Committee: Dr. Mohamad Afendee Mohamed

Signature: _____
Name of Member of
Supervisory Committee: Dr. Abdullah Bin Muhammed

Signature: _____
Name of Member of
Supervisory Committee: Associate Professor Dr. Zurina Binti Mohd Hanapi

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ADC	Analog-to-Digital Converter
AHS	Audience Human System
BCL	Basic Compression Library
CR	Compression Ratio
CPB	Cycle Per Byte
DFT	Discrete Fourier Transform
EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
ECDLP	Elliptic Curve Discret Logarithm Problem
EHCC	Embedded Harmonic Components Coding
EPE	Edge Based data Embedding
HVS	Human Vision System
HC	Huffman Coding
JPEG	Joint Photographic Experts Group
LEC	Lossless Entropy Compression
LSB	Least Significant Bit
LMS	Least Mean Square
LZW	Lempel-Ziv-Witch Algorithm
M-LZW	Modified Lempel-Ziv-Witch
MDCT	Modified Discrete Cosine Transform
MPEG	Movie Photographic Experts Group
MSE	Mean Square Error
MTE	Minimize Total Energy
OSI	Open System Interconnection
PSNR	Peak Signal-to-Noise Ratio
PVD	Pixel Value Differencing
RAM	Random Access Memory
RLE	Run Length Encoding
RPE	Random Pixel Embedding
S-LEC	Sequential Lossless Entropy Compression
S-LZW	Small Lempel-Ziv-Witch Algorithm
SHPS	Skipped High-Pass Sub-band
VOIP	Voice-Over-IP
WSN	Wireless Sensor Network

CHAPTER 1

INTRODUCTION

1.1 Introduction

In the last half a decade, the technologies of the hardware, software, and communication have been advanced in such a way that leads to the ability to build tiny wireless embedded devices loaded with unique characteristics which are called *sensors*. These microcomputers can organise themselves and communicate with each other wirelessly in a multi-hop network system to create a *Wireless Sensor Network (WSN)*, whose purposes are to sense, collect, and forward the sensed data to the users. However, to keep the sensor node small and low-cost, the sensors manufacturers have built it with a limited battery capacity and system specifications. With these limits, there are many challenges encountered with the WSN in both efficiency and security.

Working in uncensored and severe physical environment with a limited battery capacity is one of the major issues because it is difficult to recharge or change the energy resource. Furthermore, in many applications such as surveillance application, it is difficult and undesirable to replace the battery of the nodes. Hence, the sensor node may suffer from fast rate energy depletion when it runs many computing and communications operations causing sensor nodes failure. Failure of one node may cause an interruption or failure in the entire system.

The sensor nodes can get much detailed and reliable information; thus, they are widely used in critical applications such as military defence, public safety, and biomedical applications. The sensitivity of sensed data in such applications puts the WSN against various security challenges. Also, the limitation of the sensor nodes capability augments a vulnerability of the WSN to attacks. Therefore, the need increases to use a secure and efficient technique to protect the sensed data from intruders and provide confidentiality and authentication features. Designing or consummating any algorithm or protocol in the WSN should achieve many factors such as energy circumspection and security with an acceptable level of performance.

In this research work, We focus on two primary problems in WSN: the effect of message size that transmitted by the sensor nodes, and the security of those messages. The problems are tackled on two different solutions in this research. First, minimising the data size by using a suitable, efficient, and simple data compression algorithms that could accommodate the sensor node's limited resources. Next, ameliorating the security of the messages with a secure steganography solution that proposed based on one of the simplest steganography techniques.

1.2 Security and Efficiency in The WSN

Substantial attention has been acquired by the WSN in a wireless research community as envisioned solutions for many applications. Two main areas have been ame-

liorated in the WSN, which are the sensor efficiency and the security of the messages that are exchanged between sensors. The sensor nodes are restricted with limited battery capacity, memory size and low bandwidth (Zhang and Varadharajan, 2010). The lack of energy efficiency is the major challenge in the WSN because the lifetime of the network. Figure 1.1 illustrates an architecture of the major components that associated with energy consumption.

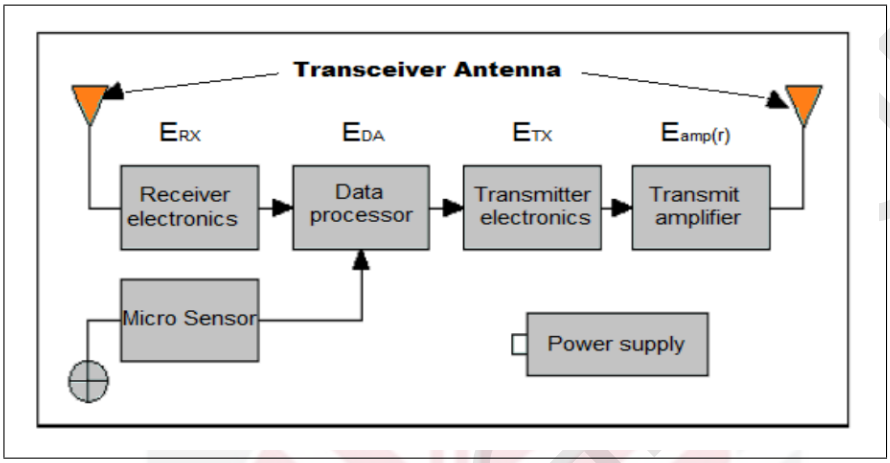

Figure 1.1: Major Components And Associated Energy Cost Parameters Of Sensor Node

The communication between sensor nodes is the most energy consuming components followed by computational operations (Hill et al., 2000). Therefore, improving the routeing algorithms or minimising the packet size has the biggest influence on the energy-efficiency amongst all ameliorative technique such as OS, access method, and network protocols improvement.

When the communication cost (energy consumption and bandwidth usage) depends mainly on the size of transmitted data, the computational effort is influenced by the security requirements (e.g. encryption, decryption, signing and data verification). Hence, to prolong the sensor node's lifetime and a whole network lifetime, these two factors have to be sustained. The amount of energy that requires for sending and receiving the messages depends mainly on the message size. The larger the message size, the more energy requires to broadcast it. Therefore, minimising the message size can significantly extend the sensor lifetime. Furthermore, it also can improve the efficiency of the data processing and decrease the computational efforts that are influenced by the input data size.

On the other hand, the security mechanism also affects the energy consumption. Securing the messages requires performing a significant amount of complex mathematical operations which consume much energy. Table 1.1 shows the main security and efficiency requirements that have to be maintained when to build a secure and efficient scheme for the WSN.

Table 1.1: Requirements of Secure and Efficient Scheme for The WSN

Requirement Type	Requirements
Efficiency Requirement	Minimum Memory Usage
	Low Computational Overhead
	Energy Efficiency
	Minimum Bandwidth Usage
Security Requirement	Authentication
	Integrity
	Fresh node addition
	Secrecy
	Resilience Against Node Capture

1.3 Problem Statement

In this thesis, several problems of interest, related to the efficiency of the sensor node, and security of the messages that are transmitted within the network is investigated. The efficiency in the WSN can be defined as the optimal resources usage for prolonging the sensor node life without affecting the performance of sensor tasks. Therefore, the research has been using two main solutions to tackle this issue either by improving the routeing protocols or minimising the transmitted data size (Lee et al., 2015; Modares et al., 2011). However, improving the routeing protocol will only affect the energy consumption during data transmission. Yet, there are other tasks also needs to be take in minds such as data processing and bandwidth usage. For that, this thesis focuses on improving efficiency of the WSN through data compression.

The problem of data size and its effects on the sensor node efficiency is studied to verify the data size effects on sensor node efficiency. The effectiveness of the sensor node is mainly associated with the size of data that is processed or transmitted. Each bit of sensed data affects the usage of system memory, computational adequacy, energy, and network bandwidth. Therefore, dealing with a raw sensed data is not an ideal solution. Decreasing the number of bits in the sensed data requires applying a compression technique, but the limitation of the sensor node limit in utilising such a technique.

The sensor network requires a practical algorithm that is not only able to compress the sensed data, but also compress a minuscule sensed information and run efficiently in the sensor node. Using current algorithms or modified lightweight algorithm, which has been proposed by (Medeiros et al., 2014), has three principal issues. First, they required a significant amount of memory space and processing power and that resulting in consuming more battery energy. Second, they are not capable of dealing with a minuscule sensed information that the sensor node generated, therefore, they cause an expansion in data size when they are used. Last, they cannot produce a high compression and decompression rate on such a limited processing power of the sensor node. These issues occur because the current algorithms are not designed specifically to work with the limitation of the sensor node and all of them are a modified variant of the traditional algorithms. Because the aforementioned reasons, we propose a new compression solution that can solve the current algorithms issues.

Secondly, we investigate the issue of transmitting messages' security when they are captured by an adversary. In many WSN applications, the sensed data is very sensitive and they are easy to be captured because of the nature and architecture of the WSN (Kaushal and Kaur, 2015). Using the invisible or secure channel to transfer the messages is practically impossible. Therefore, the messages have to be secured even if they are captured by an adversary or the network loss the main security requirements in critical applications and be insecure. Current security models are either using cryptography technique or steganography technique. Cryptography technique has been designed with a high complexity of mathematical operations to produce a high-security level. The security of the cryptographic models depends on this complex nature. Hence, these models cause many issues for the sensor node related to the efficiency and resource usage. The steganography technique has a benefit of simplicity that makes it very suitable for embedded device. However, this technique suffers from a very low-security level compared with cryptography. Therefore, in this thesis, we propose a solution to improve the security of the messages using an enhanced steganography technique without affecting the simplicity advantage.

A semi-oblivious energy aware adaptive watermarking scheme was suggested by (Imran et al., 2014) for wireless image sensor network (WISN) to secure the transmitted sensitive information. The solution is an enhancement of the original non-oblivious that was presented in (Wang et al., 2008). A low-complexity public key cryptography is used to encrypt some essential information to be transmitted with the watermarked image. The proposed solution takes into consideration the key characteristics of steganography technique such as capacity, security and imperceptibility with the WSN evaluation metrics such as computation and communication energy requirements. The number of embedding locations is evaluated with respect to two channel adaptive parameters and the impact of compression of the cover image on the correctness of extracted watermark information. The robustness of the proposed solution was investigated by statistical analysis. Furthermore, the results show that the solution can be considered relatively robust against middleman and collusion attacks. However, the solution requires minimising the additional information which is transmitted with each frame for watermarking extraction. Furthermore, the robustness of the scheme needs to be improved because the data has a very low-security level against many attacks such as brute-force attack. Therefore, we have proposed an enhanced steganography solution to improve the security of the transmitted data based on the Least Significant Bit (LSB) algorithm to preserve hiding quality and improving security against brute-force attack.

1.4 Research Objectives

The main objectives of this project are improving the efficiency and security of the WSN; therefore, we are going:

- to propose a new and efficient data compression for small data communication in the WSN. The solution can compress both small and large sensed data with the least amount of resources and energy consumption. The solution is also

fast enough to cope with the real-time applications of the WSN. Furthermore, it is simple to apply with varying types of the sensor node.

- to propose a new image-based steganographic algorithm for the WSN. The security solution is proposed based on one of the simplest steganography algorithm, which is the Least Significant Bit (LSB) algorithm. The solution is robust enough against both statistical and brute-force attacks to be able to protect the sensitive data with such attacks. Furthermore, it is suitable to work with the limited energy capacity and system resources of the sensor node.

1.5 Contributions

The following solutions are the main contributions of this thesis.

1. a novel data compression algorithm is proposed to work specifically with the sensor node and increase the efficiency of the WSN by minimising the exchanged data size. The algorithm can compress the small data as well as the large data starting from 8 bytes data size. The new compression technique is evaluated to be simple to implement, efficient in resource usage, and provide a high-performance compression so that it can be used with any sensor node platform.

2. a solution for protecting the messages that are exchanged within the network by improving the security of the LSB embedding algorithm. The solution protects the embedded messages against brute-force attack as well as the stego-analysis attacks. The steganography solution does not only can be used with the WSN but also with any computer network and applications to achieve a high-security level for the sensitive data.

1.6 Thesis Organization

The remainder of this thesis is organised as follows.

In **Chapter 2**, first, we discuss the WSN architecture, obstacles, and evaluation metrics. Then, evaluation of the current compression techniques with a review of the related work on the data compression solutions is discussed. We review the main threats and requirements of WSN security. In addition, the steganography technique is discussed with its applications, evaluation criteria, and statistical measurements. We go with further details to the LSB algorithm types, limitations and advantages. At the end of the chapter, we review the main applications of steganography techniques in the WSN with the recent solution that proposed to improve the security of the WSN by using those technologies.

In **Chapter 3**, the general research methodology that used in this thesis is explained. It presents the research framework with the exploration of each stage in details. Furthermore, it covers algorithm implementation, experiments device and data, and per-

formance metrics.

In **Chapter 4**, we introduce the new compression algorithm with a complete elucidation. Next, we provide the results of comparing the new solution with existing algorithms include the complexity, compression ratio, memory usage, number of instructions, and energy consumption.

In **Chapter 5**, we present the steganography solution with a review of an Elliptic Curve equation. After that, an examination for brute-force attack and stego-analysis is discussed.

In **Chapter 6**, we conclude the thesis and identify further directions for advancing this research.

REFERENCES

Aboelela, E. 2014. LiftingWiSe: A lifting-based efficient data processing technique in Wireless Sensor Networks. *Sensors* 14 (8): 14567–14585.

Adnan, S. F. S., Isa, M. A. M., Rahman, K. S. A., Muhamad, M. H. and Hashim, H. 2015. Simulation of RSA and ElGamal encryption schemes using RF simulator. In *Computer Applications & Industrial Electronics (ISCAIE), 2015 IEEE Symposium on*, 124–128. IEEE.

Ahmed, M., Huang, X. and Cui, H. 2013. A novel Two-Stage Algorithm Protecting Internal Attack from WSNs. *International Journal of Computer Networks & Communications* 5 (1): 97.

Ahmed, M. R., Huang, X., Sharma, D. and Cui, H. 2012. Wireless Sensor Network: Characteristics and Architectures. In *Proceedings of World Academy of Science, Engineering and Technology*, 660. World Academy of Science, Engineering and Technology (WASET).

Akbas, A., Yildiz, H. U. and Tavli, B. 2014. Data packet length optimization for Wireless Sensor Network lifetime maximization. In *Communications (COMM), 2014 10th International Conference on*, 1–6. IEEE.

Akhtar, N., Khan, S. and Johri, P. 2014. An improved inverted LSB image steganography. In *Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on*, 749–755. IEEE.

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y. and Cayirci, E. 2002a. A survey on sensor networks. *Communications magazine, IEEE* 40 (8): 102–114.

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y. and Cayirci, E. 2002b. Wireless sensor networks: a survey. *Computer networks* 38 (4): 393–422.

Al-Sharif, R., Guyeux, C., Fadil, Y. A., Makhoul, A. and Jaber, A. 2014, In Ad Hoc Networks, In *Ad Hoc Networks*, 51–62, Springer, 51–62.

Alsalaet, J. K. and Ali, A. A. 2015. Data compression in wireless sensors network using MDCT and embedded harmonic coding. *ISA transactions* 56: 261–267.

Antonopoulos, C. P. and Voros, N. S. 2015. Resource Efficient Data Compression Algorithms for Demanding, WSN based Biomedical Applications. *Journal of biomedical informatics* 59: 1–14.

Bach, E. and Shallit, J. O. 1996. *Algorithmic Number Theory: Efficient Algorithms*. , vol. 1. MIT press.

Barr, K. C. and Asanović, K. 2006. Energy-aware lossless data compression. *ACM Transactions on Computer Systems (TOCS)* 24 (3): 250–291.

Basmadjian, R. and De Meer, H. 2012. Evaluating and modeling power consumption of multi-core processors. In *Future Energy Systems: Where Energy, Computing and Communication Meet (e-Energy), 2012 Third International Conference on*, 1–10. IEEE.

Bojkovic, Z. S., Bakmaz, B. M. and Bakmaz, M. R. 2008. Security issues in wireless sensor networks. *International Journal of Communications* 2 (1): 106–115.

Boubiche, D. E., Boubiche, S., Toral-Cruz, H., Pathan, A.-S. K., Bilami, A. and Athmani, S. 2015. SDAW: secure data aggregation watermarking-based scheme in homogeneous WSNs. *Telecommunication Systems* 1–12.

Burger, W. and Burge, M. J. 2009. *Digital image processing: an algorithmic introduction using Java*. Springer Science & Business Media.

Campobello, G., Giordano, O., Segreto, A. and Serrano, S. 2015. Comparison of local lossless compression algorithms for Wireless Sensor Networks. *Journal of Network and Computer Applications* 47: 23–31.

Candès, E. J., Romberg, J. and Tao, T. 2006. Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information. *Information Theory, IEEE Transactions on* 52 (2): 489–509.

Capo-Chichi, E. P., Guyennet, H. and Friedt, J.-M. 2009. K-RLE: a new data compression algorithm for wireless sensor network. In *Sensor Technologies and Applications, 2009. SENSORCOMM'09. Third International Conference on*, 502–507. IEEE.

Cerpa, A., Elson, J., Estrin, D., Girod, L., Hamilton, M. and Zhao, J. 2001. Habitat monitoring: Application driver for wireless communications technology. *ACM SIGCOMM Computer Communication Review* 31 (2): 20–41.

Chen, W.-J., Chang, C.-C. and Le, T. H. N. 2010. High payload steganography mechanism using hybrid edge detector. *Expert Systems with applications* 37 (4): 3292–3301.

Chen, Z., Guiling, S., Weixiang, L., Yi, G. and Lequn, L. 2009. Research on Data Compression Algorithm Based on Prediction Coding for Wireless Sensor Network Nodes. In *2009 International Forum on Information Technology and Applications*, 283–286. IEEE.

Cole, E. and Krutz, R. D. 2003. *Hiding in plain sight: Steganography and the art of covert communication*. John Wiley & Sons, Inc.

Dasgupta, K., Mandal, J. and Dutta, P. 2012. Hash based least significant bit technique for video steganography (HLSB). *International Journal of Security, Privacy and Trust Management (IJSPTM)* 1 (2): 1–11.

De Clercq, R., Uhsadel, L., Van Herrewege, A. and Verbauwhede, I. 2014. Ultra low-power implementation of ECC on the ARM Cortex-M0+. In *Proceedings of the 51st Annual Design Automation Conference*, 1–6. ACM.

Dener, D. 2014. Optimum packet length over data transmission for wireless sensor networks. In *Proceedings of the 8th International Conference on Sensing Technology*, 52–56.

Díaz, Á., González, J. and Sánchez, P. 2015, In Trusted Computing for Embedded Systems, In *Trusted Computing for Embedded Systems*, 247–269, Springer, 247–269.

Ding, Q., Wang, B., Sun, X., Wang, J. and Shen, J. 2015. A Reversible Watermarking Scheme Based on Difference Expansion for Wireless Sensor Networks. *International Journal of Grid Distribution Computing* 8: 143–154.

Djebbar, F., Ayad, B., Hamam, H. and Abed-Meraim, K. 2011. A view on latest audio steganography techniques. In *Innovations in Information Technology (IIT), 2011 International Conference on*, 409–414. IEEE.

Dolfus, K. and Braun, T. 2010. An evaluation of compression schemes for wireless networks. In *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2010 International Congress on*, 1183–1188. IEEE.

Dong, X. and Li, X. 2009. An authentication method for self nodes based on watermarking in wireless sensor networks. In *Wireless Communications, Networking and Mobile Computing, 2009. WiCom'09. 5th International Conference on*, 1–4. IEEE.

Dutta, T. 2015. Medical Data Compression and Transmission in Wireless Ad Hoc Networks. *Sensors Journal, IEEE* 15 (2): 778–786.

Duy, N. T. K., Tu, N. D., Son, T. H. and Khanh, L. H. D. 2015. Automated monitoring and control system for shrimp farms based on embedded system and wireless sensor network. In *Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on*, 1–5. IEEE.

El Assi, M., Ghaddar, A., Tawbi, S. and Fadi, G. 2013. Resource-efficient floating-point data compression using MAS in WSN. *International Journal of Ad Hoc, Sensor & Ubiquitous Computing* 4 (5): 13.

Fang, J. and Potkonjak, M. 2003. Real-time watermarking techniques for sensor networks. In *Electronic Imaging 2003*, 391–402. International Society for Optics and Photonics.

Fridrich, J. 2009. *Steganography in digital media: principles, algorithms, and applications*. Cambridge University Press.

Gambhir, A. and Mishra, A. R. 2015. A New Data Hiding Technique with Multilayer Security System. *International Journal of Innovations and Advancement in Computer Science (IJIACS)* 4.

Gardner-Stephen, P., Bettison, A., Challans, R., Hampton, J., Lakeman, J. and Wallis, C. 2013. Improving Compression of Short Messages. *Int'l J. of Communications, Network and System Sciences* 2013.

Ghazanfari, K., Ghaemmaghami, S. and Khosravi, S. R. 2011. LSB++: an improvement to LSB+ steganography. In *TENCON 2011-2011 IEEE Region 10 Conference*, 364–368. IEEE.

Ghazzaal, A., Alquraishee, A. and Kar, J. 2014. A Survey on Security Mechanisms and Attacks in Wireless Sensor Networks. *International Journal for Innovative Research in Science & Technology* 7 (3): 135–147.

Ghosal, A. and Halder, S. 2015, In Cooperative Robots and Sensor Networks 2015, In *Cooperative Robots and Sensor Networks 2015*, 185–205, Springer, 185–205.

Giruka, V. C., Singhal, M., Royalty, J. and Varanasi, S. 2008. Security in wireless sensor networks. *Wireless Communications and Mobile Computing* 8 (1): 1–24.

Gupta, P. 2012. Cryptography based digital image watermarking algorithm to increase security of watermark data. *International Journal of Scientific & Engineering Research* 3 (9): 1–4.

Gupta, Ankur Goyal, S. and Bhushan, B. 2012. Information Hiding Using Least Significant Bit Steganography and Cryptography. *International Journal of Modern Education and Computer Science* 4 (6): 27–34.

Halgamuge, M. 2009. An estimation of sensor energy consumption. *Progress In Electromagnetics Research B* 12: 259–295.

Handel, T. G. and Sandford II, M. T. 1996. Hiding data in the OSI network model. In *Information Hiding*, 23–38. Springer.

Haneda, M., Knijnenburg, P. M. and Wijshoff, H. A. 2005. Automatic selection of compiler options using non-parametric inferential statistics. In *Parallel Architectures and Compilation Techniques, 2005. PACT 2005. 14th International Conference on*, 123–132. IEEE.

Hankerson, D., Menezes, A. J. and Vanstone, S. 2010. *Guide to Elliptic Curve Cryptography*. 1st edn. New York, USA: Springer Publishing Company, Incorporated.

Harjito, B. and Potdar, V. 2015. Secure Transmission in Wireless Sensor Networks Data Using Linear Kolmogorov Watermarking Technique. *arXiv preprint arXiv:1501.01376* .

Hassan, A. and Bach, C. 2014. Improving Security Connection in Wireless Sensor Networks. *International Journal of Innovation and Scientific Research* 2351–8014.

Hassanein, H. and Luo, J. 2006. Reliable energy aware routing in wireless sensor networks. In *Dependability and Security in Sensor Networks and Systems, 2006. DSSNS 2006. Second IEEE Workshop on*, 54–64. IEEE.

Hemalatha, Dinesh A, A., Renuka and Kamath, P. R. 2013. A Secure Color Image Steganography in Transform Domain. *International Journal on Cryptography and Information Security* 3 (1): 17–24.

Hill, J., Szewczyk, R., Woo, A., Hollar, S., Culler, D. and Pister, K. 2000. System architecture directions for networked sensors. *ACM SIGOPS Operating Systems Review* 34 (5): 93–104.

Huffman, D. 1952. A Method for the Construction of Minimum-Redundancy Codes. *Proceedings of the IRE* 40 (9): 1098–1101.

Hull, B., Jamieson, K. and Balakrishnan, H. 2003. Bandwidth management in wireless sensor networks. In *Proceedings of the 1st international conference on Embedded networked sensor systems*, 306–307. ACM.

Ibrahim, M. E., Rupp, M. and Habib, S.-D. 2009. Compiler-based optimizations impact on embedded software power consumption. In *Circuits and Systems and TAISA Conference, 2009. NEWCAS-TAISA'09. Joint IEEE North-East Workshop on*, 1–4. IEEE.

Imran, N., Seet, B.-C. and Fong, A. 2014. A semi-oblivious energy-aware adaptive watermarking for wireless image sensor networks. *Multimedia Systems* 20 (3): 311–326.

Jain, A. and Lakhtaria, K. 2014. A Comparative Study of Lossless Compression Algorithm on Text Data. *International Journal of Electronics and Information Engineering* 1 (1): 45–52.

Jain, R. 2012. High Capacity data hiding using LSB Steganography and Encryption. *International Journal of Engineering Science and Technology (IJEST)* 4 (6): 57–68.

Jain, Y. K. and Ahirwal, R. 2010. A novel image steganography method with adaptive number of least significant bits modification based on private stego keys. *International Journal of Computer Science and Security* 4 (1): 40–49.

Jancy, S. and Kumar, C. 2015. Packet Level Data Compression Techniques For Wireless Sensor Networks. *Journal of Theoretical and Applied Information Technology* 75 (1).

Jiang, P. and Li, S.-Q. 2010. A data compression algorithm for wireless sensor networks based on an optimal order estimation model and distributed coding. *Sensors* 10 (10): 9065–9083.

Jin, Y., Ding, Y., Hao, K. and Jin, Y. 2015. An endocrine-based intelligent distributed cooperative algorithm for target tracking in wireless sensor networks. *Soft Computing* 19 (5): 1427–1441.

Job, D. and Paul, V. 2014. Image Steganography Technique Using Sudoku Puzzle and ECC Algorithm for Secured Data Transmission. *Journal of Theoretical and Applied Information Technology* 66 (2): 447–459.

Johnson, N. F. and Jajodia, S. 1998. Exploring steganography: Seeing the unseen. *Computer* 31 (2): 26–34.

Jung, K.-H., Ha, K.-J. and Yoo, K.-Y. 2008. Image data hiding method based on multi-pixel differencing and LSB substitution methods 355–358.

Kadry, S. and Smaili, M. 2010. An improvement of RC4 cipher using vigenere cipher. *arXiv preprint arXiv:1111.5641* 1 (3): 83–92.

Kamel, I. and Juma, H. 2010. Simplified watermarking scheme for sensor networks. *International Journal of Internet Protocol Technology* 5 (1-2): 101–111.

Kamel, I. and Juma, H. 2011. A lightweight data integrity scheme for sensor networks. *Sensors* 11 (4): 4118–4136.

Karl, H. and Willig, A. 2007. *Protocols and architectures for wireless sensor networks*. John Wiley & Sons.

Kaur, S. and Verma, V. S. 2012. Design and Implementation of LZW Data Compression Algorithm. *International Journal of Information Sciences and Techniques (IJIST) Vol* 2 (4): 71–81.

Kaushal, K. and Kaur, T. 2015. A Survey on Attacks of WSN and their Security Mechanisms. *International Journal of Computer Applications* 118 (18).

Kavitha, T. and Sridharan, D. 2010. Security Vulnerabilities In Wireless Sensor Networks : A Survey. *Journal of Information Assurance and Security* 5: 31–44.

Kayalvizhi, R., Vijayalakshmi, M. and Vaidehi, V. 2010, In Recent Trends in Network Security and Applications, In *Recent Trends in Network Security and Applications*, 172–180, Springer, 172–180.

Ker, A. D. 2005. Improved detection of LSB steganography in grayscale images. In *Information Hiding*, 97–115. Springer.

Khalaf, E. T. and Sulaiman, N. 2011. A Robust Data Hiding Technique based on LSB Matching. *World Academy of Science, Engineering and Technology* 58: 117–121.

Khalifa, O. 2005. Wavelet Coding Design for Image Data Compression. *The international Arab Journal of Information Technology* 2 (2): 118–127.

Khosravi, M., Soleymanpour-Moghaddam, S. and Mahyabadi, M. 2012. Improved pair-wise LSB matching steganography with a new evaluating system. In *Telecommunications (IST), 2012 Sixth International Symposium on*, 982–986. IEEE.

Kimura, N. and Latifi, S. 2005. A survey on data compression in wireless sensor networks. In *Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on*, 8–13. IEEE.

Koc, B., Sarkar, D., Kocak, H. and Arnavut, Z. 2015. A study of power consumption on MSP432 family of microcontrollers for lossless data compression. In *High-Capacity Optical Networks and Enabling/Emerging Technologies (HONET), 2015 12th International Conference on*, 1–5. IEEE.

Kodituwakku, S. R. and Amarasinghe, U. S. 2010. Comparison of Lossless Data Compression Algorithms. *Indian Journal of Computer Science and Engineering* 1 (4): 416–425.

Kolo, J. G., Shanmugam, S. A., Lim, D. W. G., Ang, L.-M. and Seng, K. P. 2012. An adaptive lossless data compression scheme for wireless sensor networks. *Journal of Sensors* 2012: 20.

Kraus, J., Tobiska, T. and Bubla, V. 2009. Looseless encodings and compression algorithms applied on power quality datasets. *Proc. 2nd IEEE CIREDPart* 1: 1–4.

Krupa, R. R. 2014. An Overview of Image Hiding Techniques in Image Processing. *The SIJ Transactions on Computer Science Engineering & its Applications (CSEA)* 2 (2).

Ku, J., Cai, Z. and Yang, X. 2014. Hybrid Differential Evolutionary Algorithms for Koblitz Elliptic Curves Generating, 714–717. International Conference on Mechatronics, Control and Electronic Engineering.

Kumar, P. and Lee, H.-J. 2011. Security issues in healthcare applications using wireless medical sensor networks: A survey. *Sensors* 12 (1): 55–91.

Kumsawat, P., Pimpru, N., Attakitmongcol, K. and Srikaew, A. 2013. Wavelet-Based Data Compression Technique for Wireless Sensor Networks. In *Proceedings of World Academy of Science, Engineering and Technology*, 125. World Academy of Science, Engineering and Technology (WASET).

Lab, H. S. 2014, Harvard Sensor Network Lab, Volcano Mointoring (2005).

Lauter, K. 2004. The advantages of elliptic curve cryptography for wireless security. *IEEE Wireless communications* 11 (1): 62–67.

Lee, W.-S., Ahn, T.-W. and Song, C. 2015. A Study on Improvement of Energy Efficiency for LEACH Protocol in WSN. *Journal of the Institute of Electronics and Information Engineers* 52 (3): 213–220.

Leghari, M., Abbasi, S. and Dhomeja, L. D. 2010. Survey On Packet Size Optimization Techniques In Wireless Sensor Networks. In *Proceedings of the International Conference on Wireless Sensor Networks for Developing Countries (WSN4DC)*.

Leon-Salas, W. 2015. Low-complexity Compression for Sensory Systems. *IEEE Transactions on Circuits and Systems II: Express Briefs* 7747 (c): 1–1.

Li, X., Yang, B., Cheng, D. and Zeng, T. 2009. A generalization of LSB matching. *Signal Processing Letters, IEEE* 16 (2): 69–72.

Li Lei-ding, Ma Tie-hua, Y. W.-b. 2009. Analysis Of Common Lossless Compression Algorithm. *Electronic Design Engineering* 17(1): 49–53.

Liang, Y. and Li, Y. 2014. An Efficient and Robust Data Compression Algorithm in Wireless Sensor Networks. *IEEE Communications Letters* 18 (3): 439–442.

Lin, E. T. and Delp, E. J. 1999. A review of data hiding in digital images. In *PICS*, 274–278.

Lin, Q., Wang, R., Ye, N. and Wang, Z. 2013. Energy efficient distributed steganography for secure communication in wireless multimedia sensor networks. *Journal of Electronics (China)* 30 (1): 9–16.

Lipiski, B., Mazurczyk, W., Szczypiorski, K. and Śmietanka, P. 2015. Towards Effective Security Framework for Vehicular Ad-Hoc Networks. *Journal of Advances in Computer Networks* 3 (2): 134–140.

Liu, L. and Fan, G. 2003. A new JPEG2000 region-of-interest image coding method: partial significant bitplanes shift. *IEEE Signal Processing Letters* 10 (2): 35–38.

Long, S. and Xiang, P. 2012. Lossless Data Compression for Wireless Sensor Networks Based on Modified Bit-Level RLE. In *Wireless Communications, Networking and Mobile Computing (WiCOM), 2012 8th International Conference on*, 1–4. IEEE.

Lopez, Javier and Zhou, J. 2008. *Wireless Sensor Network Security*. IOS Press.

Luo, W., Huang, F. and Huang, J. 2010. Edge adaptive image steganography based on LSB matching revisited. *Information Forensics and Security, IEEE Transactions on* 5 (2): 201–214.

M Rajkamal, B. Z. 2014. Image and Text Hiding using RSA & Blowfish Algorithms with Hash-LSB Technique. *International Journal of Innovative Science, Engineering & Technology* 1 (6): 81–89.

Majeed, A., Kiah, M. L. M. M., Madhloom, H. T., Zaidan, B. B. and Zaidan, A. A. 2009. Novel approach for high secure and high rate data hidden in the image using image texture analysis. *International Journal of Engineering and Technology* 1 (2): 63–69.

Makbol, N. M. and Khoo, B. E. 2014. A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition. *Digital Signal Processing* 33: 134–147.

Mandal, B. K., Bhattacharyya, D. and Bandyopadhyay, S. K. 2013. Designing and performance analysis of a proposed symmetric cryptography algorithm. In *Communication Systems and Network Technologies (CSNT), 2013 International Conference on*, 453–461. IEEE.

Marcelloni, F. and Vecchio, M. 2008. A Simple Algorithm for Data Compression in Wireless Sensor Networks. *Communications Letters, IEEE* 12 (6): 411–413.

Marcelloni, F. and Vecchio, M. 2009. An Efficient Lossless Compression Algorithm for Tiny Nodes of Monitoring Wireless Sensor Networks. *Comput. J.* 52 (8): 969–987.

Massey, J. L. 1994. Some Applications of Source Coding in Cryptography. *European Transactions on Telecommunications* 5 (4): 421–430.

Maurya, A. K., Singh, D. and Sarje, A. K. 2011. Median predictor based data compression algorithm for Wireless Sensor Network. *International Journal of Smart Sensors and Ad Hoc Networks* 1 (1): 62–65.

Medeiros, H. P., Maciel, M. C., Demo Souza, R. and Pellenz, M. E. 2014. Lightweight Data Compression in Wireless Sensor Networks Using Huffman Coding. *International Journal of Distributed Sensor Networks* 2014: 1–11.

Min, J., Kim, J. and Kwon, Y. 2012, In Convergence and Hybrid Information Technology, In *Convergence and Hybrid Information Technology*, 9–16, Springer, 9–16.

Misbahuddin, S., Tahir, M. and Siddiqui, S. 2014. An efficient lossless data reduction algorithm for cluster based wireless sensor network. In *Collaboration Technologies and Systems (CTS), 2014 International Conference on*, 287–290. IEEE.

Modares, H., Salleh, R. and Moravejosharieh, A. 2011. Overview of security issues in wireless sensor networks. In *Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on*, 308–311. IEEE.

Mohamed, M., Al-Afari, F. and Bamatraf, M. A. M. M. 2011. Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation. *Int. Arab J. e-Technol.* 2 (1): 11–17.

Mohamed, M. A. 2014. A Survey on Elliptic Curve Cryptography. *Applied Mathematical Sciences* 8 (154): 7665–7691.

Mudgule, C. B., Nagaraj, U. and Ganjewar, P. D. 2015. Data Compression in Wireless Sensor Network: A Survey. *International Journal of Innovative Research in Computer and Communication Engineering* 2: 6664–6673.

Munir, A., Gordon-Ross, A. and Ranka, S. 2014. Multi-core embedded wireless sensor networks: Architecture and applications. *IEEE Transactions on Parallel and Distributed Systems* 25: 1553–1562.

Neeta, D., Snehal, K. and Jacobs, D. 2006. Implementation of LSB steganography and its evaluation for various bits. In *Digital Information Management, 2006 1st International Conference on*, 173–178. IEEE.

Nelson, M. and Gailly, J.-L. 1996. *The data compression book*. 2nd edn. M&T Books New York.

Pallister, J., Hollis, S. J. and Bennett, J. 2015. Identifying compiler options to minimize energy consumption for embedded platforms. *The Computer Journal* 58 (1): 95–109.

Paul, S. and Preneel, B. 2004. A New Weakness in the RC4 Keystream Generator and an Approach to Improve the Security of the Cipher. In *Fast Software Encryption*, 245–259. Springer.

Pereira, R. 1998, IP payload compression using DEFLATE, Tech. rep.

Petrou, M. and Petrou, C. 2010. *Image processing: the fundamentals*. 2nd edn. John Wiley & Sons.

Potlapally, N. R., Ravi, S., Raghunathan, A. and Jha, N. K. 2006. A study of the energy consumption characteristics of cryptographic algorithms and security protocols. *Mobile Computing, IEEE Transactions on* 5 (2): 128–143.

Pradhan, S. S., Kusuma, J. and Ramchandran, K. 2002. Distributed compression in a dense microsensor network. *Signal Processing Magazine, IEEE* 19 (2): 51–60.

Praveena, N., LANJEWAR, D. U. A. and Babu, C. M. 2013. Viable Network Intrusion Detection on Wireless Adhoc Networks. *International Journal of Computers & Technology* 5 (1): 29–34.

Pu, I. M. 2005. *Fundamental Data Compression*. Butterworth-Heinemann.

Rahman, K. C. 2010. A survey on sensor network. *Journal of Computer and Information Technology* 1 (1): 76–87.

Raja, K., Chowdary, C., Venugopal, K. and Patnaik, L. 2005. A secure image steganography using LSB, DCT and compression techniques on raw images. In *Intelligent Sensing and Information Processing, 2005. ICISIP 2005. Third International Conference on*, 170–176. IEEE.

Ramachandran, S., Sridhar, U., Srinivasan, V. and Jothi, J. J. 2011. Data Aggregation and Privacy for Police Patrols. *arXiv preprint arXiv:1107.4054* 2 (2): 51–62.

Rane, S. D. and Sapiro, G. 2001. Evaluation of JPEG-LS, the new lossless and controlled-lossy still image compression standard, for compression of high-resolution elevation data. *Geoscience and Remote Sensing, IEEE Transactions on* 39 (10): 2298–2306.

Rao, B. S., Prashanthi, M. and Kumar, G. P. 2012. Implementation Of WLAN WEP Protocol By RC4 Algorithm In VHDL. *International Journal Of Engineering Science Advanced Technology* 2 (4): 1090–1095.

Reddy, H. S. M. and Raja, K. B. 2009. High capacity and security steganography using discrete wavelet transform. *International Journal of Computer Science and Security (IJCSS)* 3 (6): 462.

Rein, S., Gühmann, C. and Fitzek, F. 2006. Compression of short text on embedded systems. *Journal of Computers* 1 (6): 1–10.

Reinhardt, A., Christin, D., Hollick, M., Schmitt, J., Mogre, P. S. and Steinmetz, R. 2010, In Wireless Sensor Networks, In *Wireless Sensor Networks*, 33–48, Springer, 33–48.

Ren, X. and Yu, H. 2006. Security mechanisms for wireless sensor networks. *IJCSNS International Journal of Computer Science and Network Security* 6 (3): 155–156.

Robles, R. J. and Choi, M.-K. 2009, In Security Technology, In *Security Technology*, 289–297, Springer, 289–297.

Ruangchaijatupon, N. and Krishnamurthy, P. 2001. Encryption and power consumption in wireless LANs. In *The Third IEEE workshop on wireless LANS*, 148–152.

Sadler, C. M. and Martonosi, M. 2006. Data compression algorithms for energy-constrained devices in delay tolerant networks. In *Proceedings of the 4th international conference on Embedded networked sensor systems*, 265–278. ACM.

Sandilya, M. and Chawla, M. 2014, Spatial Domain Image Steganography based on Security and Randomization.

Santini, S. and Romer, K. 2006. An adaptive strategy for quality-based data reduction in wireless sensor networks. In *Proceedings of the 3rd international conference on networked sensing systems (INSS 2006)*, 29–36.

Santoso, A. J., Nugroho, L., Suparta, G. and Hidayat, R. 2011. Compression Ratio and Peak Signal to Noise Ratio in Grayscale Image Compression using Wavelet. *International Journal of Computer Science and Technology* 2 (2): 7–11.

Sasikumar, P., Vivek, C. and Jayakrishnan, P. 2010. Key-Management Systems in Vehicular Ad-Hoc Networks. *International Journal of Computer Applications* 10 (1): 23–28.

Schonberg, D., Ramchandran, K. and Pradhan, S. S. 2004. Distributed code constructions for the entire Slepian-Wolf rate region for arbitrarily correlated sources. In *Data Compression Conference, 2004. Proceedings. DCC 2004*, 292–301. IEEE.

Schoof, R. 1985. Elliptic curves over finite fields and the computation of square roots mod P. *Mathematics of Computation* 44 (170): 483–494.

Sculley, D. and Brodley, C. E. 2006. Compression and machine learning: A new perspective on feature space vectors. In *Data Compression Conference, 2006. DCC 2006. Proceedings*, 332–341. IEEE.

Seng, J. S. and Tullsen, D. M. 2003. The effect of compiler optimizations on Pentium 4 power consumption. In *Interaction Between Compilers and Computer Architectures, 2003. INTERACT-7 2003. Proceedings. Seventh Workshop on*, 51–56. IEEE.

Shahina Sheikh, M. H. D. 2015. Data Compression Techniques for Wireless Sensor Network. *International Journal of Computer Science and Information Technologies(IJSIT)* 6: 818–821.

Shaik, A. K., Kumar, C. A. and Saheb, M. 2015. Implementation of Wireless Sensor Networks for Industrial Applications Using The Multi-Core Architecture. *International Journal of Engineering Research and Applications (IJERA) ISSN:* (January): 8–12.

Shanmugasundaram, S. and Lourdusamy, R. 2011. A comparative study of text compression algorithms. *International Journal of Wisdom Based Computing* 1 (December): 68–76.

Shannon, C. 1948. A Mathematical Theory of Communication. *The Bell System Technical Journal,* 27 (July 1948): 379–423.

Sharma, M. 2010. Compression using Huffman coding. *IJCSNS International Journal of Computer Science and Network Security* 10 (5): 133–141.

Sharma, N., Kaur, J., Kaur, N., Sharma, N., Kaur, J. and Kaur, N. 2014. A Review on various Lossless Text Data Compression Techniques. *International Journal of Engineering Sciences* 2 (December): 58–63.

Shukla, C. P. and Singh, A. K. 2014. Secure Communication with the help of Encryption in Video Steganography. *Current Trends in Technology and Sciences* 3 (6): 408–410.

Sidhu, A. S. and Garg, E. M. 2014. Research Paper on Text Data Compression Algorithm using Hybrid Approach. *CSE & Guru Kashi University, Talwandi Sabo, Bathinda, Punjab* 3 (12): 1–10.

Singh, S. K., Singh, M. and Singh, D. 2011. A survey on network security and attack defense mechanism for wireless sensor networks. *International Journal of Computer Trends and Technology* 1 (2): 9–17.

Singla, D. and Juneja, M. 2014. An analysis of edge based image steganography techniques in spatial domain. In *Engineering and Computational Sciences (RAECS), 2014 Recent Advances in*, 1–5. IEEE.

Song, W. 2013. Strategies and Techniques for Data Compression in Wireless Sensor Networks. *TELKOMNIKA Indonesian Journal of Electrical Engineering* 11 (11): 6624–6630.

Sora, D. 2010. Security Issues in Wireless Sensor Networks. *International Journal of Online Engineering (iJOE)* 6 (4): pp–26.

Specs, I. A. P. 2015, ARK | Your Source for Intelő Product Information.

Srisooksai, T., Keamarungsi, K., Lamsrichan, P. and Araki, K. 2012. Practical data compression in wireless sensor networks: A survey. *Journal of Network and Computer Applications* 35 (1): 37–59.

Stolikj, M., Cuijpers, P. J. and Lukkien, J. J. 2012. Energy-aware reprogramming of sensor networks using incremental update and compression. *Procedia Computer Science* 10: 179–187.

Strydis, C. and Gaydadjiev, G. N. 2008. Profiling of lossless-compression algorithms for a novel biomedical-implant architecture. In *Proceedings of the 6th IEEE/ACM/IFIP international conference on Hardware/Software codesign and system synthesis*, 109–114. ACM.

Suarjaya, I. M. A. D. 2012. A new algorithm for data compression optimization. *IJACSA) International Journal of Advanced Computer Science and Applications* 3 (8).

Sudha, M. N. and Valarmathi, M. L. 2011. Low Power Consumption with Optimal Two Hop In Wireless Sensor Networks. In *International Conference on Future Information Technology*, 285–288. Singapore.

Sujae, P. R. and Selvaraju, S. 2014. Power Efficient Adaptive Compression Technique for Wireless Sensor Networks. *Middle-East Journal of Scientific Research* 20 (10): 1286–1291.

Sun, X., Su, J., Wang, B. and Liu, Q. 2013. Digital watermarking method for data integrity protection in wireless sensor networks. *International Journal of Security and Its Applications* 7 (4): 407–416.

Swain, G. and Lenka, S. K. 2015. A novel steganography technique by mapping words with LSB array. *International Journal of Signal and Imaging Systems Engineering* 8 (1-2): 115–122.

Szczechowiak, P., Oliveira, L. B., Scott, M., Collier, M. and Dahab, R. 2008, In Wireless sensor networks, In *Wireless sensor networks*, 305–320, Springer, 305–320.

Tao, H., Zain, J. M., Ahmed, M. M., Abdalla, A. N. and Jing, W. 2012. A wavelet-based particle swarm optimization algorithm for digital image watermarking. *Integrated Computer-Aided Engineering* 19 (1): 81–91.

Tarrant, A. 1976. Color in Business, Science and Industry. *Journal of Modern Optics* 23 (4): 340–340.

Tharini, C. and Ranjan, P. V. 2009. Design of modified adaptive Huffman data compression algorithm for wireless sensor network. *Journal of Computer Science* 5 (6): 466.

Valverde, J., Otero, A., Lopez, M., Portilla, J., De La Torre, E. and Riesgo, T. 2012. Using SRAM based FPGAs for power-aware high performance wireless sensor networks. *Sensors* 12 (3): 2667–2692.

Verdone, R., Dardari, D., Mazzini, G. and Conti, A. 2010. *Wireless sensor and actuator networks: technologies, analysis and design*. Academic Press.

Verma, D., Jain, R. and Shrivastava, A. 2015. Performance Analysis of Cryptographic Algorithms RSA and ECC in Wireless Sensor Networks. *IUP Journal of Telecommunications* 7 (3): 51–65.

Viswanatham, V. M. and Manikonda, J. 2010. A novel technique for embedding data in spatial domain. *International Journal on Computer Science and Engineering, IJCSE* 2 (2010).

Vitter, J. S. 1987. Design and analysis of dynamic Huffman codes. *Journal of ACM (JACM)* 34 (4): 825–845.

Wang, B., Qian, H., Sun, X., Shen, J. and Xie, X. 2015a. A Secure Data Transmission Scheme Based on Information Hiding in Wireless Sensor Networks. *International Journal of Security and Its Applications* 9 (1): 125–138.

Wang, B., Su, J., Zhang, Y., Wang, B., Shen, J., Ding, Q. and Sun, X. 2015b. A Copyright Protection Method for Wireless Sensor Networks Based on Digital Watermarking. *International Journal of Hybrid Information Technology* 8 (6): 257–268.

Wang, F. and Liu, J. 2011. Networked wireless sensor data collection: issues, challenges, and approaches. *Communications Surveys & Tutorials, IEEE* 13 (4): 673–687.

Wang, H. 2013. Communication-resource-aware adaptive watermarking for multimedia authentication in wireless multimedia sensor networks. *The Journal of Supercomputing* 64 (3): 883–897.

Wang, H., Peng, D., Wang, W., Sharif, H. and Chen, H.-H. 2008. Energy-aware adaptive watermarking for real-time image delivery in wireless sensor networks. In *Communications, 2008. ICC'08. IEEE International Conference on*, 1479–1483. IEEE.

Wang, H. and Wang, S. 2004. Cyber warfare: steganography vs. steganalysis. *Communications of the ACM* 47 (10): 76–82.

Wu, H., Abouzeid, A. et al. 2004. Power aware image transmission in energy constrained wireless networks. In *Computers and communications, 2004. Proceedings. ISCC 2004. Ninth international symposium on*, 202–207. IEEE.

Wu, H.-t., Dugelay, J.-L. and Cheung, Y.-m. 2008. A data mapping method for steganography and its application to images. In *Information Hiding*, 236–250. Springer.

Xia, N., Feng, R. and Xu, L. 2012, In Wireless Algorithms, Systems, and Applications, In *Wireless Algorithms, Systems, and Applications*, 112–119, Springer, 112–119.

Xiao, J.-J., Cui, S., Luo, Z.-Q. and Goldsmith, A. J. 2006. Power scheduling of universal decentralized estimation in sensor networks. *Signal Processing, IEEE Transactions on* 54 (2): 413–422.

Xiao, R., Sun, X. and Yang, Y. 2008. Copyright protection in wireless sensor networks by watermarking. In *Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP'08 International Conference on*, 7–10. IEEE.

Xiao, S., Gong, W. and Towsley, D. 2010. Secure wireless communication with dynamic secrets. In *INFOCOM, 2010 Proceedings IEEE*, 1–9. IEEE.

Xiao, X., Sun, X., Yang, L. and Chen, M. 2007. Secure data transmission of wireless sensor network based on information hiding. In *Mobile and Ubiquitous Systems: Networking & Services, 2007. MobiQuitous 2007. Fourth Annual International Conference on*, 1–6. IEEE.

Yan-li, Z., Xiao-ping, F., Shao-qiang, L. and Zhe-yuan, X. 2010. Improved LZW algorithm of lossless data compression for WSN. In *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on*, 523–527. IEEE.

Yang, H., Sun, X. and Sun, G. 2009. A high-capacity image data hiding scheme using adaptive LSB substitution. *Radioengineering* 18 (4): 509.

Ye, F., Zhong, G., Cheng, J., Lu, S. and Zhang, L. 2003. PEAS: A robust energy conserving protocol for long-lived sensor networks. In *Distributed computing systems, 2003. Proceedings. 23rd international conference on*, 28–37. IEEE.

Yin, Y., Liu, F., Zhou, X. and Li, Q. 2015. An Efficient Data Compression Model Based on Spatial Clustering and Principal Component Analysis in Wireless Sensor Networks. *Sensors* 15 (8): 19443–19465.

Yoon, M., Jang, M., Kim, H.-I. and Chang, J.-W. 2014. A signature-based data security technique for energy-efficient data aggregation in wireless sensor networks. *International Journal of Distributed Sensor Networks* 2014: 10–pp.

ZainEldin, H., Elhosseini, M. A. and Ali, H. A. 2014. Image compression algorithms in wireless multimedia sensor networks: A survey. *Ain Shams Engineering Journal* 6 (2): 481–490.

Zhang, J. and Varadharajan, V. 2010. Wireless sensor network key management survey and taxonomy. *Journal of Network and Computer Applications* 33 (2): 63–75.

Zhang, W., Liu, Y., Das, S. K. and De, P. 2008. Secure data aggregation in wireless sensor networks: a watermark based authentication supportive approach. *Pervasive and Mobile Computing* 4 (5): 658–680.

Zhi, L. and Fen, S. A. 2004. Detection of random LSB image steganography. In *Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th*, 2113–2117. IEEE.

Zhou, Y., Fang, Y. and Zhang, Y. 2008. Securing wireless sensor networks: a survey. *Communications Surveys & Tutorials, IEEE* 10 (3): 6–28.